Service Description:

Cisco Subscription Services for Network Authentication

(CON-AS-NETAUTH)

This document describes Cisco's Subscription Service for Network Authentication.

Related Documents: This document should be read in conjunction with the following documents also posted at www.cisco.com/go/servicedescriptions/ : (1) Glossary of Terms; (2) List of Services Not Covered; and (3) Severity and Escalation Guidelines. All capitalized terms in this description have the meaning ascribed to them in the Glossary of Terms.

Direct Sale from Cisco. If you have purchased these Services directly from Cisco, this document is incorporated into your Master Services Agreement (MSA) or equivalent services agreement executed between you and Cisco. In the event of a conflict between this Service Description and your MSA or equivalent services agreement, this Service Description shall govern.

Sale from Cisco Authorized Reseller. If you have purchased these Services through a Cisco Authorized Reseller, this document is for description purposes only; is not a contract between you and Cisco. The contract, if any, governing the provision of this Service will be the one between you and your Cisco Authorized Reseller. Your Cisco Authorized Reseller should provide this document to you or you can obtain a copy of this and other Cisco service descriptions at www.cisco.com/go/servicedescriptions/.

Cisco shall provide the Network Authentication Services described below as selected and detailed on the Purchase Order for which Cisco has been paid the appropriate fee. Cisco shall provide a Quote for Services ("Quote") setting out the extent of the Services that Cisco shall provide and the period during which such Services shall be provided. Cisco shall receive a Purchase Order that references the Quote agreed between the parties and that, additionally, acknowledges and agrees to the terms contained therein.

Cisco Subscription Service for Network Authentication

Service Summary

Net Authenticate is a Cisco Advanced Services targeted at identifying counterfeit hardware and grey market components in Customer's network. This service engagement is focused on reducing risk posed by having these types of devices operating in the network. The Net Authenticate service enables Cisco to provide Customer with the extra assurance that the products in the network are genuine Cisco products.

The **Cisco Assessment Service for Network Authentication** ("Net Authenticate Service") relies on a suite of software tools, processes, and product data forensics that enables Cisco to proactively collect and analyze Customer inventory data, and provide information back to the Customer.

The Service analyzes the types of product families and sub-families ("Covered Devices"). Covered Devices are defined at the Cisco serial number level or Cisco Product IDs ("PID") that exist within a chassis. A detailed list of Covered Devices is available upon request.

The Service supports discovery of up to a specific quantity of devices defined in the Quote over an annual duration, at specific collection locations listed in the Quote, and includes up to a specific number of trips for a Cisco Network Consulting Engineer (NCE) to travel on-site to perform required duties. The Service includes executive summary reports of findings.

Service Methodology

The Net Authenticate Service is focused on validating the authenticity of the Customer's Cisco product and requires a data collection process, which requires Cisco capturing relevant device inventory data via proprietary collection tools. Alternatively, the Customer can collect the inventory on their behalf, subject to Cisco agreeing to the collection process and data format, and transmit to Cisco for analysis.

The data collection process is typically performed in two steps:

1. Network Discovery process to identify covered Cisco branded hardware on the network. (Credentials information required).

2. Inventory process to collect data elements from each device discovered in the network. Customer Network Information is processed and stored to enable generation of authenticity reports. These reports will be provided to the Customer upon completion of the Network Discovery and Inventory process.

The Service leverages the software from the hardware device to validate authenticity. Hardware validation might be required later for further confirmation.

Authenticity checks include the following:

- **Genuine Product**: Based on provided data, nothing suspicious was found when the Cisco product was inventoried and analyzed by the Net Authenticate Service and has been identified by Cisco as being a genuine Cisco product, which can be placed under a service contract.
- **Counterfeit Product:** Based on the provided data, the device was not built by Cisco, or was materially altered post manufacture without Cisco's consent, and in Cisco's opinion, was generally produced with the intent to counterfeit or imitate a genuine Cisco product.
- **Authorized Product**: Based on provided device and Customer details, the device and associated software license were originally sold to the intended end user or the associated software license were transferred to the end user in accordance with the Cisco Software Transfer and Re-licensing Policy.
- **Grey Market Product**: Based on provided data, the device and associated software license were originally sold to another end customer. Device warranty typically does not transfer with such sales and standard Cisco policy dictates equipment inspection and relicensing is required prior to addition to any maintenance service contact such as SMARTnet.
- **Unresolved/Open questions**: Based on provided data, the device cannot be analyzed. Common causes for this assessment result include, but are not limited to, the following: missing information in the data collection, and no product serial number present in the data collection.
- **Missing Product Sales Data**: Full and complete sales data for the collected serial number is not available. This can be caused when sales records originate from older transactions or when Point of Sale (POS) data has been either unreported or inaccurately reported to Cisco

Deliverables

The Net Authenticate Service provides the following set of deliverables:

- Executive Summary Report

- Detailed Report of Findings

Cisco Responsibilities

Cisco shall provide services during Standard Business Hours (unless stated otherwise) for the duration of the services term identified in the Quote:

General Support

- Schedule project kick-off meeting and review high-level requirements for data collection.
- Conduct regular status calls.
- Provide the Request For Information (RFI) questionnaire to Customer, which contains a list of Covered Devices, which may be updated from time to time, that Cisco will perform the assessment against.
- Review the Customer response to the RFI questionnaire for any applicable follow-up questions or clarifications.
- Use the Customer response as input for planning the performance of the analysis and device authentication.
- Work with Customer to review Cisco data collector deployment requirements.

Net Authenticate Analysis and Assessment

Cisco will perform the authentication analysis, up to an amount specified in the Quote, of Customer's network, collecting device information to assess authenticity and the activities will be performed:

- Set up and configure data collection tools based on the Customer requirements. Data collection will occur in one of the following means:
    - Cisco Service Platform Collection (CSPC)
    - NetformX (third party collection software)
    - Manual Data Collection (Cisco-approved, Customer performed collection)
- Perform data collection from Covered Devices on the Customer network.
- Analyze collected data and complete the Net Authenticate Summary which outlines findings, remediation recommendations, and includes executive summary report(s), addressing Counterfeit Product, Genuine Product, Authorized Product and Grey Market Product(s) found in the collection.

Knowledge Transfer

- Create Executive Summary slide deck for the presentation in the onsite session.
- Provide for Customer stakeholders an Executive Summary presentation and schedule a session on site for up to four (4) hours to include information on the device discovery.

Customer Responsibilities

- Complete the RFI questionnaire.
- Provide all information as requested by Cisco to be documented in the RFI questionnaire within five (5) Business Days following receipt of the RFI questionnaire.
- Designate key contacts and authorized personnel including network architects, system/application administrators and IT engineers who shall be available for on-going information gathering and feedback during the Service.
- Provide full details related to the following:
    - Current network topology, including access, distribution, and core layers, types of switches, routers, and firewalls;
    - Internet Protocol (IP) addressing and sub-netting for each device planned to be managed along with SNMP Read community strings and device credentials;

  - Features and services that have been enabled on the network.
  - Current IT management solutions and devices managed

- Participate in the project kick off meeting providing representation from applicable technical teams.
- In the event Customer elects to perform a manual data or scripted data collection of the network inventory, approval must be obtained from Cisco with the content and data format requirements communicated by Cisco.
- Rack, stack, power-up, and install operating system, applying any operating system patches and connecting the server to the network.
- Perform any required configuration tasks.
- Ensure connection of all applicable referenced cards, line cards and transceivers into a supported router or switch intended to be authenticated.
- Review the Acceptance Test Plan document with Cisco if one is created.
- Participate in the execution of the Acceptance Test Plan and provide any applicable feedback if one is created.
- Schedule the necessary facilities for onsite Acceptance Testing including conference rooms, projectors, and network connectivity for Cisco resource.
- Designate up to five (5) Customer stakeholders to participate in the Executive Summary Reporting.
- Work with Cisco to schedule the Executive Summary Reporting, scheduling the necessary facilities for the presentation, including conference rooms, projectors, and network connectivity, if required.
- All information (such as but not limited to: designs, topologies, requirements) provided by Customer is assumed to be up-to-date and valid for the Customer's current environment. Cisco Services are based upon information provided to Cisco by Customer at the time of the Services.
- Customer acknowledges that the completion of Services is dependent upon Customer meeting its responsibilities as indicated herein.
- Identify Customer's personnel and define their roles in the participation of the Services. Such personnel may include but is not limited to: architecture design and planning engineers, and network engineers.
- Ensure Customer's personnel are available to participate during the course of the Services to provide information and to participate in scheduled information gathering sessions, interviews, meetings and conference calls.
- Support services provided by Cisco comprise technical advice, assistance and guidance only.

Limitations and Disclaimers

- Any Report provided by Cisco under this Service will be delivered directly to Customer regardless of whether Service was purchased directly by Customer or resold by a Cisco authorized reseller to Customer.
- Cisco may use and store Customer's network information obtained through performance of the Net Authenticate Services at Cisco's discretion for commercial and business purposes. Cisco will use reasonable commercial efforts to protect the data and any Customer identifying information.
- Any Covered Device discovered and identified as Counterfeit is not entitled to receive support by Cisco and Cisco recommends that Customer discontinue use of such product(s) identified as Counterfeit.
- Cisco shall not be responsible for the failure of the Net Authenticate Services to meet Customer's network, design, business, or other requirements. In no event shall Cisco be liable for the accuracy or completeness of the information contained in any reporting, including as a result of Missing Product Sales Data or other information provided in connection with the Net Authenticate Services.